

## COMPUTER ILLEGAL USE PREVENTION DEVICE

Publication number: JP9171416

Publication date: 1997-06-30

Inventor: SUZUKI HITOSHI; UEHARA MINORU; FURUYUI AKIO

Applicant: HITACHI LTD

Classification:

- international: G06F1/00; G06F12/14; G06F15/00; G06F21/20;  
G06F1/00; G06F12/14; G06F15/00; G06F21/20; (IPC1-7): G06F1/00; G06F15/00

- European:

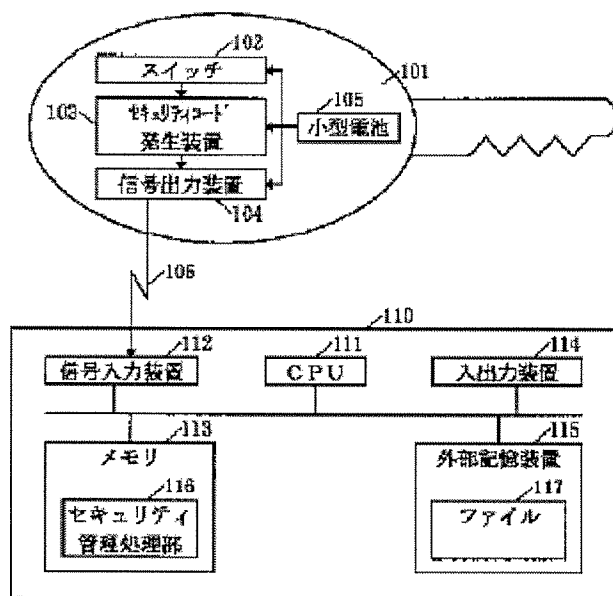
Application number: JP19960212276 19960812

Priority number(s): JP19960212276 19960812; JP19950271161 19951019

Report a data error here

### Abstract of JP9171416

**PROBLEM TO BE SOLVED:** To improve the operability of a security management preventing computer illegal use by providing a security key with a signal output device outputting a security code and providing a security management processing part executing and permitting a function when a security code signal is inputted and this signal is a valid security code on a computer main body. **SOLUTION:** This device is provided with a security key 101, a switch 102, a security code generator 103, a signal output device 104, a small-sized battery 105, a security code signal 106, a computer 110, a CPU 111, a signal input device 112, a memory 113, an input/output device 114, an external storage 115, a security control processing part 116 and a file 117. Unique codes are preliminarily stored in a read only memory, etc., provided on a security code generator 103 and these codes are generated as security codes.



Data supplied from the esp@cenet database - Worldwide



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-171416

(43) 公開日 平成9年(1997)6月30日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 1/00	3 7 0		G 0 6 F 1/00	3 7 0 E
15/00	3 3 0		15/00	3 3 0 G

審査請求 未請求 請求項の数 3 O L (全 20 頁)

(21) 出願番号 特願平8-212276

(22) 出願日 平成8年(1996)8月12日

(31) 優先権主張番号 特願平7-271161

(32) 優先日 平7(1995)10月19日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 鈴木 仁

神奈川県海老名市下今泉810番地 株式会

社日立製作所オフィスシステム事業部内

(72) 発明者 上原 実

神奈川県海老名市下今泉810番地 株式会

社日立製作所オフィスシステム事業部内

(72) 発明者 古結 明男

神奈川県海老名市下今泉810番地 株式会

社日立製作所オフィスシステム事業部内

(74) 代理人 弁理士 秋田 収喜

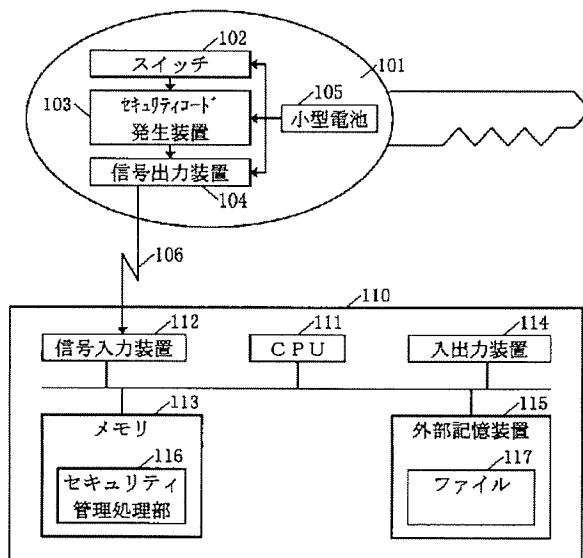
(54) 【発明の名称】 コンピュータ不正使用防止装置

(57) 【要約】

【課題】 コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能な技術を提供する。

【解決手段】 ユニークなセキュリティコードを発生するセキュリティコード発生装置と、前記セキュリティコードをセキュリティコード信号に変換して前記セキュリティコードを出力する信号出力装置とをセキュリティキーに備え、前記セキュリティコード信号を入力して前記セキュリティコードに変換する信号入力装置と、前記変換されたセキュリティコードと登録リストに登録された複数の有効なセキュリティコードとを比較し、前記変換されたセキュリティコードが有効なセキュリティコードである場合に前記セキュリティコードに対応する機能の実行を許可するセキュリティ管理処理部とをコンピュータ本体に備えるものである。

図 1



**【特許請求の範囲】**

【請求項1】 非接触型または接触型のセキュリティキーを利用したコンピュータの不正使用を防止するコンピュータ不正使用防止装置であって、

ユニークなセキュリティコードを発生するセキュリティコード発生装置と、前記セキュリティコードをセキュリティコード信号に変換して前記セキュリティコードを出力する信号出力装置とをセキュリティキーに備え、前記セキュリティコード信号を入力して前記セキュリティコードに変換する信号入力装置と、前記変換されたセキュリティコードと登録リストに登録された複数の有効なセキュリティコードとを比較し、前記変換されたセキュリティコードが有効なセキュリティコードである場合に前記セキュリティコードに対応する機能の実行を許可するセキュリティ管理処理部とをコンピュータ本体に備えることを特徴とするコンピュータ不正使用防止装置。

【請求項2】 コンピュータ本体からの信号を入力する信号入力装置をセキュリティキーに備え、セキュリティキーに信号を出力する信号出力装置をコンピュータ本体に備えることを特徴とする請求項1に記載されたコンピュータ不正使用防止装置。

【請求項3】 ネットワークを介してセキュリティコードを送信するセキュリティコード送信部と、ネットワークを介して送信されたセキュリティコードを受信するセキュリティコード受信部とをネットワークに接続された複数のコンピュータ本体に備え、特定のコンピュータのセキュリティコード送信部からネットワークに接続された他のコンピュータのセキュリティコード受信部にセキュリティコードを送信し、前記送信したセキュリティコードを使用して前記他のコンピュータのセキュリティ管理処理を実行することを特徴とする請求項1または請求項2のいずれかに記載されたコンピュータ不正使用防止装置。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、非接触型または接触型のセキュリティキーによりコンピュータの不正使用を防止するコンピュータ不正使用防止装置に関し、特に、セキュリティキーから送られたセキュリティコードに応じてコンピュータの特定の機能の実行を許可するコンピュータ不正使用防止装置に適用して有効な技術に関するものである。

**【0002】**

【従来の技術】近年、コンピュータを使用した業務が増加するにつれて、会社の機密に関するデータや個人のプライバシーに関するデータ等、機密保護を必要とする多量のデータがコンピュータに蓄積されてきている。

【0003】従来のコンピュータに蓄積されたデータの機密保護に関しては、「電子情報通信ハンドブック、電子情報通信学会編」等に記載されており、コンピュータ

に蓄積されたデータの暗号化、コンピュータの利用者の利用資格の確認を行うユーザ認証、データが改ざんされていないことを確認するデータ認証及び記憶装置上の他のプログラムやデータを保護する記憶保護がある。

【0004】前記従来のコンピュータに蓄積されたデータの機密保護の内、コンピュータの利用者の利用資格を確認し、コンピュータの不正使用を防止するユーザ認証には、(a)パスワードを使用する方法、(b)フロッピーディスクやPCカードなどの取り外し可能な記憶媒体を用いる方法、(c)磁気カード等の専用入出力装置を必要とする記憶媒体を用いる方法、及び、(d)物理的な鍵を使用する方法がある。

【0005】前記(a)のパスワードを使用する方法は、利用者を識別するユーザIDと利用者本人しか知ることのできないパスワードをコンピュータ内に格納し、利用者がコンピュータを使用する際に、その利用者のユーザIDとパスワードを入力し、入力されたパスワードと前記コンピュータ内に格納されているパスワードとを比較し、入力されたパスワードが前記コンピュータ内に格納されているパスワードと一致するときに、そのパスワードを入力した利用者が正規の利用者本人であるとみなす方法である。

【0006】前記(b)のフロッピーディスクやPCカードなどの取り外し可能な記憶媒体を用いる方法は、利用者がコンピュータに装着したフロッピーディスクやPCカード等の取り外し可能な記憶媒体に格納されたデータを読み出し、そのデータが予めコンピュータ内部に格納されているデータと一致するときに、その記憶媒体を装着した利用者が正規の利用者本人であるとみなす方法である。

【0007】前記(c)の磁気カード等の専用入出力装置を必要とする記憶媒体を用いる方法は、利用者の磁気カード等の記憶媒体に格納されたデータを専用入出力装置によって読み出し、その読み出したデータが予めコンピュータ内部に格納されているデータと一致するときに、その記憶媒体を所持している利用者が正規の利用者本人であるとみなす方法である。

【0008】前記(d)の物理的な鍵を使用する方法は、コンピュータを設置した部屋やコンピュータの電源スイッチ等を物理的な鍵を使用して施錠し、前記コンピュータを使用する際には、物理的な鍵を使用してコンピュータを設置した部屋やコンピュータの電源スイッチ等の施錠を解除する方法である。

**【0009】**

【発明が解決しようとする課題】本発明者は、前記従来技術を検討した結果、以下の問題点を見出した。

【0010】すなわち、前記(a)のパスワードを使用する方法では、コンピュータの利用者がパスワードをメモ用紙に記録したり、他の人に記憶してもらったり、記憶しやすいコードにすることがある為、パスワードが利

用者本人以外に漏洩しやすいという問題があった。

【0011】また、前記(a)のパスワードを使用する方法では、異なるユーザIDで同じパスワードを使用することができる為、パスワードは必ずしもユニークとはならず、偶然に漏洩する可能性があるという問題があった。

【0012】前記(a)のパスワードを使用する方法で、定期的にパスワードを切り替えることによりパスワードの漏洩を防止した場合には、漏洩はしにくくなるもののパスワードを忘れる可能性は更に高くなるという問題があった。

【0013】前記(b)のフロッピーディスクやPCカード等の取り外し可能記憶媒体を用いる方法では、コンピュータのフロッピーディスクやPCカードの装着スロットがコンピュータの不正使用を防止するセキュリティキーとしての用途に占有され、他の用途に使用できなくなるという問題と、フロッピーディスクやPCカードを装着スロットに頻繁に装着することにより摩耗が発生し、フロッピーディスクやPCカードのデータを読み取る信頼性が低下したり、フロッピーディスクやPCカードを装着スロットに装着したまま忘れて他の人に盗難されたり、そのままコンピュータを不正に使用されてしまう危険性が高いという問題があった。

【0014】また、フロッピーディスクは携帯は可能であるが、自動車の鍵や家の鍵の様に常に身に付けておくには不便であると共に複製が容易である為、漏洩しやすいという問題があり、PCカードは他の記憶媒体と比較して高価な為、現用のキーの他に予備のキーを設けたり、1台のコンピュータを複数の利用者で共用する為に複数のセキュリティキーを設けたり、コンピュータの管理の為に管理者用のキーと利用者用のキーの様に複数のセキュリティキーを設けたりする場合に、他の記憶媒体よりも多くの費用がかかるという問題があった。

【0015】前記(c)の磁気カード等の専用入出力装置が必要な記憶媒体を用いる方法では、コンピュータに専用入出力装置を接続する必要がある為、多くの費用がかかるという問題と、ノート型コンピュータなど携帯性を生かしたコンピュータでは専用入出力装置の接続により携帯性が著しく損なわれてしまうという問題があった。

【0016】前記(d)の物理的な鍵を使用する方法では、鍵を装着したまま忘れて他の人に盗難されたり、そのままコンピュータを不正に使用されてしまう危険性が高いという問題と、鍵の複製が簡単な反面、現用のキーを無効化し予備のキーに切り替えることや、1台のコンピュータを複数の利用者で共用する為に複数のセキュリティキーを設けたり、コンピュータの管理の為に管理者用のキーと利用者用のキーの様に複数のセキュリティキーを設けたりするのが困難であるという問題があった。

【0017】本発明の目的は、コンピュータの不正使用

を防止するセキュリティ管理の操作性を向上することが可能な技術を提供することにある。

【0018】本発明の他の目的は、セキュリティの強度を向上させることが可能な技術を提供することにある。

【0019】本発明の他の目的は、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュータに対してもセキュリティ管理を行うことが可能な技術を提供することにある。

【0020】本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明かになるであろう。

【0021】

【課題を解決するための手段】本願によって開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【0022】(1)非接触型または接触型のセキュリティキーを利用したコンピュータの不正使用を防止するコンピュータ不正使用防止装置であって、ユニークなセキュリティコードを発生するセキュリティコード発生装置と、前記セキュリティコードをセキュリティコード信号に変換して前記セキュリティコードを出力する信号出力装置とをセキュリティキーに備え、前記セキュリティコード信号を入力して前記セキュリティコードに変換する信号入力装置と、前記変換されたセキュリティコードと登録リストに登録された複数の有効なセキュリティコードとを比較し、前記変換されたセキュリティコードが有効なセキュリティコードである場合に前記セキュリティコードに対応する機能の実行を許可するセキュリティ管理処理部とをコンピュータ本体に備えるものである。

【0023】前記コンピュータ不正使用防止装置では、まず、前記セキュリティキーのスイッチを押すことにより、前記セキュリティコード発生装置からユニークなセキュリティコードを発生する。

【0024】次に、前記セキュリティキーの信号出力装置は、前記発生したセキュリティコードを特定のセキュリティコード信号、例えば、赤外線信号に変換し、前記変換したセキュリティコード信号をコンピュータの信号入力装置に出力する。

【0025】このとき、前記セキュリティキーのセキュリティコード発生装置及び信号出力装置への給電は、前記セキュリティキーに備えられた小型電池によって行われる。

【0026】前記コンピュータの信号入力装置は常時予備電源により動作し、前記セキュリティキー側の信号出力装置から送られてきたセキュリティコード信号を、コンピュータ側の信号入力装置で入力してセキュリティコードに変換する。

【0027】次に、前記コンピュータのセキュリティ管理処理部は、予め有効なセキュリティコードを登録した登録リストを参照し、前記変換したセキュリティコード

と前記登録リスト中のセキュリティコードとを比較して、前記変換したセキュリティコードが有効なセキュリティコードであるかどうかの照合判定を行う。

【0028】前記変換したセキュリティコードが有効なセキュリティコードである場合には、前記セキュリティコードに対応する特定の機能の実行を許可し、また、前記変換したセキュリティコードが有効なセキュリティコードでない場合には、前記コンピュータの使用を禁止する。

【0029】前記変換したセキュリティコードが有効なセキュリティコードである場合に許可する機能としては、コンピュータ本体の主電源の投入、以前ロックされた入力操作の再開、前記コンピュータ内の情報に対する参照、移動、複写、変更、暗号化及び復号化の操作等が挙げられる。

【0030】前記コンピュータ不正使用防止装置のセキュリティキーは、ユニークなセキュリティコードを発生するセキュリティコード発生装置と、例えば、今後のコンピュータでは標準的に装備される赤外線インタフェースを備えた信号出力装置と、前記セキュリティコード発生装置及び信号出力装置に電源を供給する小型電池と、スイッチとから構成することにより、小型で低コストかつ非接触型とすることが可能である。

【0031】前記の様に、コンピュータに標準的に装備される赤外線インタフェースを使用することにより、コンピュータのフロッピーディスク等の装着スロットの専用機器による占有や前記専用機器搭載によるコストアップを伴うことなく、コンピュータの不正使用を防止することが可能である。

【0032】また、セキュリティキーを小型で低コストにし、コンピュータ本体への専用機器搭載によるコストアップをなくしたことから、予備のセキュリティキー、1台のコンピュータを複数の利用者で共用する際の複数のセキュリティキー、または、コンピュータの管理を行う際に使用する管理者用セキュリティキーと管理以外の処理の際に使用する利用者用セキュリティキーの様に用途別の複数のセキュリティキーを設けることが容易である。

【0033】以上の様に、前記コンピュータ不正使用防止装置によれば、発生したユニークなセキュリティコードを出力してコンピュータのセキュリティ管理を行うので、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能である。

【0034】(2)前記(1)に記載されたコンピュータ不正使用防止装置において、コンピュータ本体からの信号を入力する信号入力装置をセキュリティキーに備え、セキュリティキーに信号を出力する信号出力装置をコンピュータ本体に備えるものである。

【0035】前記コンピュータ不正使用防止装置では、例えば、ICカードで構成されたセキュリティキーのセ

キュリティコード発生装置から発生されたユニークなセキュリティコードを特定のセキュリティコード信号に変換し、前記変換したセキュリティコード信号をコンピュータの信号入力装置に出力する。

【0036】前記コンピュータの信号入力装置は、前記セキュリティキー側の信号出力装置から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、前記コンピュータのセキュリティ管理処理部は、登録リストを参照して、前記変換したセキュリティコードが有効なセキュリティコードであるかどうかの照合判定を行う。

【0037】前記変換したセキュリティコードが有効なセキュリティコードである場合には、前記セキュリティコードに対応する特定の機能の実行を許可し、また、前記変換したセキュリティコードが有効なセキュリティコードでない場合には、前記コンピュータの使用を禁止する。

【0038】前記セキュリティ管理処理部は、前記変換したセキュリティコードが有効なセキュリティコードである場合に、セキュリティコードを変更する機能が選択されると、前記登録リスト中のセキュリティコードを変更すると共に、前記コンピュータの信号出力装置により、前記変更したセキュリティコードをセキュリティコード信号に変換してセキュリティキーに出力する。

【0039】前記セキュリティキーの信号入力装置は、前記コンピュータ本体側の信号出力装置から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、前記変換したセキュリティコードを使用してセキュリティキーのセキュリティコード発生装置が発生するセキュリティコードを変更する。

【0040】また、前記の様にICカードを使用してセキュリティキーを高機能化し、コンピュータ本体の信号出力装置及びセキュリティキーの信号入力装置を使用することにより、コンピュータ本体の使用履歴情報や障害情報をセキュリティキーに蓄積したり、また、セキュリティ管理だけでなく、勤怠情報を蓄積して勤怠管理に使用したり、製品情報を蓄積して在庫管理に使用し、また、現金情報を蓄積して電子マネーと兼用することが可能である。

【0041】以上の様に、前記コンピュータ不正使用防止装置によれば、コンピュータの信号出力装置により変更したセキュリティコードをセキュリティキーに出力し、セキュリティキーのセキュリティコードを変更するので、セキュリティの強度を向上せさせることが可能である。

【0042】(3)前記(1)または(2)に記載されたコンピュータ不正使用防止装置において、ネットワークを介してセキュリティコードを送信するセキュリティコード送信部と、ネットワークを介して送信されたセキュリティコードを受信するセキュリティコード受信部と

をネットワークに接続された複数のコンピュータ本体に備え、特定のコンピュータのセキュリティコード送信部からネットワークに接続された他のコンピュータのセキュリティコード受信部にセキュリティコードを送信し、前記送信したセキュリティコードを使用して前記他のコンピュータのセキュリティ管理処理を実行するものである。

【0043】前記コンピュータ不正使用防止装置では、セキュリティキーから受信したセキュリティコードが有効なセキュリティコードである場合に、他のコンピュータのセキュリティ管理を実行する機能が選択されると、前記セキュリティコード送信部により、前記セキュリティキーから受信済みの有効なセキュリティコードをネットワークに接続された他のコンピュータに送信する。

【0044】前記ネットワークに接続された他のコンピュータは、セキュリティコード受信部によりセキュリティコードを受信した後、当該コンピュータのセキュリティ管理処理部を起動する。

【0045】前記セキュリティコード送信部によりセキュリティコードを送信したコンピュータは、前記起動された他のコンピュータのセキュリティ管理処理部に、セキュリティ管理に関する指示を送り、当該コンピュータのセキュリティ管理機能を実行する。

【0046】以上の様に、前記コンピュータ不正使用防止装置によれば、ネットワークに接続された他のコンピュータのセキュリティ管理処理を実行するので、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュータに対してもセキュリティ管理を行うことが可能である。

【0047】

【発明の実施の形態】

（実施形態1）以下に、本発明のコンピュータ不正使用防止装置において、赤外線非接触型セキュリティキーを使用する実施形態1のコンピュータ不正使用防止装置について説明する。

【0048】図1は、本実施形態のコンピュータ不正使用防止装置の概略構成を示す図である。図1において、101はセキュリティキー、102はスイッチ、103はセキュリティコード発生装置、104は信号出力装置、105は小型電池、106はセキュリティコード信号、110はコンピュータ、111はCPU、112は信号入力装置、113はメモリ、114は入出力装置、115は外部記憶装置、116はセキュリティ管理処理部、117はファイルである。

【0049】図1に示す様に、本実施形態のコンピュータ不正使用防止装置は、セキュリティキー101と、スイッチ102と、セキュリティコード発生装置103と、信号出力装置104と、小型電池105と、セキュリティコード信号106と、コンピュータ110と、CPU111と、信号入力装置112と、メモリ113

と、入出力装置114と、外部記憶装置115と、セキュリティ管理処理部116と、ファイル117とを有している。

【0050】また、図1に示す様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティキー101として、小型、低コストで、キーホルダー等に付け、常にコンピュータ110の管理者の身に付けて不便のないものが作成可能であり、複数のセキュリティキー101を作成することにより、1個を現用セキュリティキー、他を予備セキュリティキーとして用意することが低コストで可能になる。

【0051】本実施形態のコンピュータ不正使用防止装置では、セキュリティコード発生装置103に備えられたリードオンリメモリ等に予めユニークなコードを記憶しておき、これをセキュリティコードとして発生させており、ユニークなコードと変化するコード、例えば日付時刻などを合成したコードをセキュリティコードとして使用することにより、セキュリティコード信号106の不正な複製を困難にすることが可能である。

【0052】本実施形態のコンピュータ不正使用防止装置の信号出力装置104及び信号入力装置112は、今後のパーソナルコンピュータで標準的に装備される赤外線インタフェース（IrDA: Infra red Data Association）を使用し、また、セキュリティ管理処理部116は、パスワードによるセキュリティの管理機能と同様にソフトウェアで実現する。

【0053】本実施形態のコンピュータ不正使用防止装置では、ユニークなセキュリティコードを発生するセキュリティコード発生装置103、赤外線インタフェースを持つ信号入力装置112、小型電池105及びスイッチ102により、セキュリティキー101を小型、低コストかつ非接触型とし、コンピュータ110のフロッピーディスク等の装着スロットの専用機器による占有や前記専用機器搭載によるコストアップをなくしている。

【0054】この為、本実施形態のコンピュータ不正使用防止装置では、予備セキュリティキーや、1台のコンピュータ110を複数の利用者で共用する際に様にセキュリティキー101を複数としたり、また、コンピュータ110の管理の際に使用する管理者用セキュリティキーと管理以外の処理に使用する利用者用セキュリティキーの様にセキュリティキー101を複数設けることが容易である。

【0055】更に、本実施形態のコンピュータ不正使用防止装置では、1人の利用者が複数台のコンピュータ110を操作あるいは管理する場合には、複数台のコンピュータ110に対して1つのセキュリティキー101を共通に登録することも可能である。

【0056】図2は、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116の概略構成を示す図である。図2において、201は登録処理機

能、202は変更処理機能、203はシステム起動ロック処理機能、204は中断再開ロック処理機能、205はアプリケーション起動ロック処理機能、206はファイルロック処理機能、207は暗号化処理機能、208は復号化処理機能、209は使用状況の履歴取得処理機能、210は登録リストである。

【0057】図2に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116は、登録処理機能201と、変更処理機能202と、システム起動ロック処理機能203と、中断再開ロック処理機能204と、アプリケーション起動ロック処理機能205と、ファイルロック処理機能206と、暗号化処理機能207と、復号化処理機能208と、使用状況の履歴取得処理機能209と、登録リスト210とを有している。

【0058】また、図2に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116では、登録リスト210に登録された内容により、対応する処理機能の実行を管理している。

【0059】登録処理機能201は、登録リスト210にセキュリティコードが登録されていない場合、登録リスト210にセキュリティキー101からのセキュリティコードを登録する機能であり、複数のセキュリティコードの登録や、セキュリティキー101ごとに有効範囲、すなわち、当該セキュリティコードによって実行できるセキュリティ管理処理部116の機能の範囲、およびコンピュータ操作環境（画面環境、ファイル環境、アプリケーション環境等）の登録を行う機能である。

【0060】変更処理機能202は、登録リスト210にセキュリティコードが既に登録されている場合に登録リスト210に登録されている有効なセキュリティコードを受信すると、登録リスト210の変更を許可する機能であり、例えばセキュリティコードの追加登録、登録抹消、有効範囲の変更、コンピュータ操作環境等の変更を行う機能である。

【0061】システム起動ロック処理機能203は、登録リスト210にセキュリティコードが登録されているときに、登録リスト210に登録されている有効なセキュリティコードが受信されない場合にはコンピュータ110の電源の投入及びシステム起動を禁止し、有効なセキュリティコードが受信された場合には、そのセキュリティコードに対応して予め設定したコンピュータ操作環境への切り替えを行う機能である。

【0062】中断再開ロック処理機能204は、登録リスト210にセキュリティコードが登録されているときに、一定時間中に入出力装置114のキーボードやマウス等からの入力無く、コンピュータ110への操作が行われなかった場合に、コンピュータ110への操作が中断されているとみなして入出力装置114のディスプレイの画面を消去し、入出力装置114のキーボードや

マウス等からの入力動作をロックし、登録リスト210に登録されている有効なセキュリティコードを受信するまでコンピュータ110の入出力装置114からの入力動作を中断する機能である。

【0063】アプリケーション起動ロック処理機能205は、登録リスト210にセキュリティコードが登録されている場合に、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内の予め設定されたアプリケーションソフトウェアを起動しようとしたときに、登録リスト210に登録されている有効なセキュリティコードを受信するまでの間、当該アプリケーションソフトウェアの起動を停止する機能である。

【0064】ファイルロック処理機能206は、登録リスト210にセキュリティコードが登録されている場合に、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内の予め設定されたファイル117に対して参照、移動、複写、変更などの操作を行おうとしたときに、登録リスト210に登録されている有効なセキュリティコードを受信するまでの間、ファイル117への操作を停止する機能である。

【0065】暗号化処理機能207は、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内のファイル117や通信電文などを暗号化するとき、セキュリティキー101からのセキュリティコードに基づいて暗号化を行う機能である。

【0066】復号化処理機能208は、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内の暗号化されたファイル117や通信電文などを復号化するとき、セキュリティキー101からのセキュリティコードに基づいて復号化を行う機能である。

【0067】使用状況の履歴取得処理機能209は、登録リスト210にセキュリティコードが登録されている場合に、登録リスト210に登録されている有効なセキュリティコードを受信していない間のコンピュータ110の使用状況の履歴を記憶する機能である。

【0068】図3は、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの登録処理の処理手順を示すフローチャートである。

【0069】図3に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの登録処理では、ステップ301の処理で、コンピュータ110のセキュリティ管理処理部116の登録処理機能201を呼び出し、セキュリティコードの登録処理機能201を起動する。

【0070】ステップ302の処理で、セキュリティキー101の信号出力装置104から送信されたセキュリティコード信号106をコンピュータ110の信号入力装置112で受信し、ステップ303の処理で、受信したセキュリティコード信号106をセキュリティコードに変換して登録リスト210に登録する。



【0071】ステップ304の処理では、ステップ303の処理で登録したセキュリティコードに、当該セキュリティコードで実行できるセキュリティ管理処理部116を示す有効範囲を設定する。この有効範囲の設定により、コンピュータ110を管理する管理者と一般の利用者とをそのセキュリティコードによって区別し、実行できるセキュリティ管理処理部116を受信されたセキュリティコードに応じて変更する。

【0072】ステップ305の処理では、ステップ303の処理で登録したセキュリティコードに、当該セキュリティコードを受信したときのコンピュータ操作環境を設定する。このコンピュータ操作環境の設定により、コンピュータ110でセキュリティコードを受信してコンピュータ110の使用を開始したときに、コンピュータ110の操作環境を受信したセキュリティコードに応じて特定の操作環境に変更する。

【0073】複数のセキュリティコードを登録する場合には、ステップ306の処理で、次のセキュリティキー101の信号出力装置104からコンピュータ110の信号入力装置112へ、次のセキュリティコード信号106を送信し、登録リスト210に登録し、以下これを繰り返す。

【0074】本実施形態のコンピュータ不正使用防止装置において、前記の様にセキュリティコードの登録処理を行うと、登録リスト210には、「セキュリティコード1」、「セキュリティコード2」等の複数のセキュリティコードと、各セキュリティコードに対応する「処理機能1」、「処理機能2」等の複数の処理機能が登録される。

【0075】ここで、登録リスト210に登録される「処理機能1」、「処理機能2」等の複数の処理機能の内容は、対応するセキュリティコードが入力されたときに実行可能な複数の処理機能を有効範囲として示すと共に、当該処理機能を実行する際の操作環境を表しているものとする。

【0076】本実施形態のコンピュータ不正使用防止装置では、手元にあるセキュリティキー101からのセキュリティコード信号106を直接コンピュータ110に送信して登録するので、誤って違うコードを登録してしまうミスを防止することが可能である。

【0077】図4は、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの変更処理の処理手順を示すフローチャートである。

【0078】図4に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティコードの変更処理では、ステップ401の処理で、コンピュータ110のセキュリティ管理処理部116の変更処理機能202を呼び出し、セキュリティコードの変更処理機能202を起動する。

【0079】ステップ402の処理で、セキュリティキ

ー101の信号出力装置104から送信したセキュリティコード信号106をコンピュータ110の信号入力装置112で受信し、ステップ403の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較する。

【0080】ステップ403の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードである場合には、コンピュータ110のセキュリティ管理処理部116は、登録リスト210の変更を許可する。

【0081】ステップ404の処理で、セキュリティコードを追加登録する処理を選択した場合には、ステップ414の処理に進み、追加したいセキュリティキー101の信号出力装置104からコンピュータ110の信号入力装置112へセキュリティコード信号106を送信し、送信されたセキュリティコードを登録リスト210に登録する。登録リスト210に追加登録されたセキュリティコードには、セキュリティコードごとに有効範囲やコンピュータ操作環境を設定することが可能である。

【0082】ステップ405の処理で、セキュリティコードの登録抹消を行う処理を選択した場合には、ステップ415の処理に進み、登録抹消したいセキュリティコードを指定して登録リスト210から消去する。

【0083】ステップ406の処理で、セキュリティコードの有効範囲を変更する処理を選択した場合には、ステップ416の処理に進み、有効範囲を変更したいセキュリティコードを指定し、変更した有効範囲を登録リスト210に登録しなおす。

【0084】ステップ407の処理で、セキュリティコードに対応するコンピュータ操作環境を変更する処理を選択した場合には、ステップ417の処理に進み、コンピュータ操作環境を変更したいセキュリティコードを指定し、設定を変更したコンピュータ操作環境を登録リスト210に登録しなおす。

【0085】ステップ403の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードではない場合には、登録リスト210の変更は許可されない。

【0086】以上の様に、本実施形態のコンピュータ不正使用防止装置では、コンピュータ110に複数のセキュリティコードを登録する機能と登録したセキュリティコードの内容を変更する機能とを備えているので、セキュリティキー101が不正に使用された場合に不正に使用されたセキュリティキー101を無効化することが可能である。

【0087】また、本実施形態のコンピュータ不正使用

防止装置では、コンピュータ110のセキュリティキー101毎に有効範囲を設定する機能と前記の設定した有効範囲を変更する機能とを備えているので、管理者と利用者でセキュリティのレベルを変更することが可能である。

【0088】図5は、本実施形態のコンピュータ不正使用防止装置のシステム起動ロック処理の処理手順を示すフローチャートである。

【0089】図5に示す様に、本実施形態のコンピュータ不正使用防止装置のシステム起動ロック処理では、ステップ501の処理で、セキュリティキー101の信号出力装置104から送信したセキュリティコード信号106を、補助電源で動作中のコンピュータ110の信号入力装置112で受信し、ステップ502の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較する。

【0090】ステップ502の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードである場合には、ステップ503の処理に進み、主電源を投入した後、ステップ504の処理に進み、コンピュータ110のシステム起動を行う。

【0091】ステップ502の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードではない場合には、主電源の投入及びシステム起動は行わない。

【0092】前記の様に、本実施形態のコンピュータ不正使用防止装置によれば、セキュリティ管理処理部116のシステム起動ロック処理機能203により、有効なセキュリティキー101がない場合には、コンピュータ110のパワーオン及びシステム起動が行えないので、コンピュータ110の盗難等による不正使用を防止することが可能である。

【0093】また、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部116の機能のシステム起動ロック処理機能203により、有効なセキュリティコードを受信するとコンピュータ110のパワーオン及びシステム起動が行なわれ、有効なセキュリティコードに対応して予め設定したコンピュータ操作環境に切り替えるので、コンピュータ110の操作環境をセキュリティコードに対応した利用者ごとの使いやすい操作環境に切り替えることが可能である。

【0094】図6は、本実施形態のコンピュータ不正使用防止装置の中断再開ロック処理の処理手順を示すフローチャートである。

【0095】図6に示す様に、本実施形態のコンピュータ不正使用防止装置の中断再開ロック処理では、ステッ

プ601の処理で、一定時間中に入出力装置114のキーボードまたはマウス等への入力が行われているかを調べ、入出力装置114への入力が行われていない場合には、ステップ602の処理に進み、入出力装置114のディスプレイの画面を消去した後、ステップ603の処理で、入出力装置114のキーボードやマウス等からの入力を停止する。

【0096】ステップ604の処理で、セキュリティキー101の信号出力装置104から送信されたセキュリティコード信号106を、コンピュータ110の信号入力装置112で受信し、ステップ605の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較する。

【0097】ステップ605の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードである場合には、ステップ606の処理に進み、入出力装置114のディスプレイの画面表示を再開した後、ステップ607の処理に進み、入出力装置114のキーボードやマウス等からの入力を受け付ける。

【0098】ステップ605の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードではない場合には、ステップ604の処理に戻る。

【0099】前記の様に、本実施形態のコンピュータ不正使用防止装置によれば、セキュリティ管理処理部116の中断再開ロック処理機能204により、有効なセキュリティキー101がない場合には、中断されたコンピュータ110の入出力装置114からの入力動作の再開が行えないので、コンピュータ110の利用者が不在時または離席時に不正使用されることを防止することが可能である。

【0100】図7は、本実施形態のコンピュータ不正使用防止装置のアプリケーション起動ロック処理の処理手順を示すフローチャートである。

【0101】図7に示す様に、本実施形態のコンピュータ不正使用防止装置のアプリケーション起動ロック処理では、ステップ701の処理で、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内のアプリケーションソフトウェアを起動する起動要求が行われると、ステップ702の処理で、セキュリティキー101の信号出力装置104から送信されたセキュリティコード信号106をコンピュータ110の信号入力装置112で受信し、ステップ703の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較する。

【0102】ステップ703の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードである場合には、ステップ704の処理に進み、ステップ701の処理で起動要求が行われているアプリケーションソフトウェアの起動を行う。

【0103】ステップ703の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードではない場合には、ステップ701の処理で起動要求が行われているアプリケーションソフトウェアの起動を行わない。

【0104】図8は、本実施形態のコンピュータ不正使用防止装置のファイルロック処理の処理手順を示すフローチャートである。

【0105】図8に示す様に、本実施形態のコンピュータ不正使用防止装置のファイルロック処理では、ステップ801の処理で、コンピュータ110の外部記憶装置115内あるいはネットワークで接続された他のコンピュータ内に格納されているファイル117を操作するファイル操作要求が行われると、ステップ802の処理で、セキュリティキー101の信号出力装置104から送信されたセキュリティコード信号106をコンピュータ110の信号入力装置112で受信し、ステップ803の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較する。

【0106】ステップ803の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードである場合には、ステップ804の処理に進み、ステップ801の処理でファイル操作要求が行われているファイル117への操作を実行する。

【0107】ステップ803の処理で、受信したセキュリティコードと登録リスト210に登録されているセキュリティコードとを比較した結果、受信したセキュリティコードが登録リスト210に登録されている有効なセキュリティコードではない場合には、ステップ801の処理でファイル操作要求が行われているファイル117への操作を実行しない。

【0108】前記の様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部116の機能のファイルロック処理機能206により、有効なセキュリティキー101がない場合には、ファイル117の操作が行えなくなり、有効なセキュリティコードを受信した後にファイル操作要求を実行するので、コンピュータ110内のファイル117の不正使用を防止するこ

とが可能である。

【0109】図9は、本実施形態のコンピュータ不正使用防止装置の暗号化処理の処理手順を示すフローチャートである。

【0110】図9に示す様に、本実施形態のコンピュータ不正使用防止装置の暗号化処理では、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内のファイル117や通信電文などを暗号化するときに、ステップ901の処理で、コンピュータ110のセキュリティ管理処理部116の暗号化処理機能207を呼び出し、暗号化処理機能207を起動する。

【0111】ステップ902の処理で、セキュリティキー101の信号出力装置104から送信されたセキュリティコード信号106をコンピュータ110の信号入力装置112で受信し、ステップ903の処理で、受信したセキュリティコードに基づいて暗号化処理を実行する。

【0112】図10は、本実施形態のコンピュータ不正使用防止装置の復号化処理の処理手順を示すフローチャートである。

【0113】図10に示す様に、本実施形態のコンピュータ不正使用防止装置の復号化処理では、コンピュータ110内あるいはネットワークで接続された他のコンピュータ内の暗号化されたファイル117や通信電文などを復号化するときに、ステップ1001の処理で、コンピュータ110のセキュリティ管理処理部116の復号化処理機能208を呼び出し、復号化処理機能208を起動する。

【0114】ステップ1002の処理で、セキュリティキー101の信号出力装置104から送信されたセキュリティコード信号106をコンピュータ110の信号入力装置112で受信し、ステップ1003の処理で、受信したセキュリティコードに基づいて復号化処理を実行する。

【0115】前記の様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部116の暗号化処理機能207と復号化処理機能208とにより、コンピュータ110内の情報の暗号化及び復号化を行うので、コンピュータ110内およびネットワーク等で接続された他のコンピュータ内のデータやアプリケーションソフトウェア等の情報の不正使用を防止することが可能である。

【0116】図11は、本実施形態のコンピュータ不正使用防止装置の使用状況の履歴取得処理の処理手順を示すフローチャートである。

【0117】図11に示す様に、本実施形態のコンピュータ不正使用防止装置の使用状況の履歴取得処理では、ステップ1101の処理で、入出力装置114からの入力が行われたときに、ステップ1102の処理で、登録リスト210に登録されている有効なセキュリティコー

ドを受信済みであるかどうかを調べる。

【0118】ステップ1102の処理で、登録リスト210に登録されている有効なセキュリティコードを受信済みであるかどうかを調べた結果、有効なセキュリティコードが受信されていない場合には、ステップ1101の処理で入出力装置114に入力された内容を、コンピュータ110の使用状況の履歴として、コンピュータ110の外部記憶装置115内あるいはネットワークで接続された他のコンピュータ内の履歴ファイルに記憶する。

【0119】前記の様に、本実施形態のコンピュータ不正使用防止装置では、セキュリティ管理処理部116の機能の使用状況の履歴取得処理機能209により、有効なセキュリティキー101がない場合には、コンピュータ110の使用状況の履歴を記憶するので、コンピュータ110の不正使用を行おうとする操作が全て記録されることを示すことにより、コンピュータ110の不正使用を直接防止するのではなく、コンピュータ110の不正使用を行おうとする試みを抑止することが可能である。

【0120】また、本実施形態のコンピュータ不正使用防止装置では、セキュリティキー101のセキュリティコードをネットワーク通信におけるアクセス元を認証する為のワンタイムパスワードとして応用することにより、ネットワークを使用した不正な通信を防止することが可能である。

【0121】すなわち、ネットワークを使用してアクセスするアクセス元は、このネットワークから初めにアクセス元に送られた固定的でないコードとアクセス元のセキュリティコードと間で一定の計算を行った結果、例えば、イクスクルーシブオアを行った計算結果をそのアクセスに使用するパスワードとし、ネットワーク側は、このパスワードと初めに送ったコード間でさらにイクスクルーシブオアの計算を行えば、セキュリティコードを得ることができ、アクセス元を認証することが可能である。このとき、ネットワークから初めに送られるコードは毎回変わる為、アクセスに使用するパスワードも毎回変わり、そのパスワードが盗聴されても不正に使用することができない。

【0122】以上説明した様に、本実施形態のコンピュータ不正使用防止装置によれば、発生したユニークなセキュリティコードを出力してコンピュータのセキュリティ管理を行うので、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能である。

【0123】（実施形態2）以下に、本発明のコンピュータ不正使用防止装置において、ＩＣカードのセキュリティキーを使用する実施形態2のコンピュータ不正使用防止装置について説明する。

【0124】図12は、本実施形態のコンピュータ不正使用防止装置の概略構成を示す図である。図12におい

て、1200はセキュリティキー、1201はＩＣカード側信号入力装置、1210はＩＣカードリーダライタ、1211はＩＣカードリーダライタ側信号出力装置である。

【0125】図12に示す様に、本実施形態のコンピュータ不正使用防止装置は、セキュリティキー1200と、ＩＣカード側信号入力装置1201と、ＩＣカードリーダライタ1210と、ＩＣカードリーダライタ側信号出力装置1211とを有している。

【0126】また、図12に示す様に、本実施形態のコンピュータ不正使用防止装置では、ＩＣカードであるセキュリティキー1200を使用して、コンピュータ110のセキュリティ管理を行う。

【0127】本実施形態のコンピュータ不正使用防止装置のセキュリティキー1200は、コンピュータ110から出力されるセキュリティコード等の情報を入力するＩＣカード側信号入力装置1201に備えており、また、コンピュータ110のＩＣカードリーダライタ1210は、セキュリティキー1200にセキュリティコード等の情報を出力するＩＣカードリーダライタ側信号出力装置1211を備えている。

【0128】図13は、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116の概略構成を示す図である。図13において、1301はセキュリティコード変更処理機能である。

【0129】図13に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116は、セキュリティコード変更処理機能1301を有している。

【0130】本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116は、実施形態1に示した複数の処理機能に加え、登録リスト210に登録された特定のセキュリティコードと、セキュリティキー1200に記憶されているセキュリティコードとを同時に変更するセキュリティコード変更処理機能1301を備えている。

【0131】本実施形態のコンピュータ不正使用防止装置では、ＩＣカードで構成されたセキュリティキー1200のセキュリティコード発生装置103から発生されたユニークなセキュリティコードを特定のセキュリティコード信号に変換し、前記変換したセキュリティコード信号をコンピュータ110のＩＣカードリーダライタ1210の信号入力装置112に出力する。

【0132】コンピュータ110の信号入力装置112は、セキュリティキー1200の信号出力装置104から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、コンピュータ110のセキュリティ管理処理部116は、登録リスト210を参照して、前記変換したセキュリティコードが有効なセキュリティコードであるかどうかの照合判定を行う。

【0133】前記変換したセキュリティコードが有効なセキュリティコードである場合には、前記セキュリティコードに対応する特定の機能の実行を許可し、また、前記変換したセキュリティコードが有効なセキュリティコードでない場合には、前記コンピュータ110の使用を禁止する。

【0134】また、セキュリティ管理処理部116は、前記変換したセキュリティコードが有効なセキュリティコードである場合に、セキュリティコードを変更するセキュリティコード変更処理機能1301が選択されると、登録リスト210中の対応するセキュリティコードを変更すると共に、コンピュータ110のICカードリーダーライタ側信号出力装置1211により、前記変更したセキュリティコードをセキュリティコード信号に変換してセキュリティキー1200に出力する。

【0135】セキュリティキー1200のICカード側信号入力装置1201は、コンピュータ110のICカードリーダーライタ側信号出力装置1211から送られてきたセキュリティコード信号を入力してセキュリティコードに変換し、前記変換したセキュリティコードを使用してセキュリティキー1200のセキュリティコード発生装置103が発生するセキュリティコードを変更する。

【0136】また、前記の様にICカードを使用してセキュリティキー1200を高機能化し、コンピュータ110のICカードリーダーライタ側信号出力装置1211及びセキュリティキー1200のICカード側信号入力装置1201を使用することにより、コンピュータ110の使用履歴情報や障害情報をセキュリティキー1200に蓄積したり、また、セキュリティ管理だけでなく、勤怠情報を蓄積して勤怠管理に使用したり、製品情報を蓄積して在庫管理に使用し、また、現金情報を蓄積して電子マネーと兼用することが可能である。

【0137】以上説明した様に、本実施形態のコンピュータ不正使用防止装置によれば、コンピュータの信号出力装置により変更したセキュリティコードをセキュリティキーに出力し、セキュリティキーのセキュリティコードを変更するので、セキュリティの強度を向上せさることが可能である。

【0138】（実施形態3）以下に、本発明のコンピュータ不正使用防止装置において、ネットワークに接続された他のコンピュータのセキュリティ管理を行う実施形態3のコンピュータ不正使用防止装置について説明する。

【0139】図14は、本実施形態のコンピュータ不正使用防止装置の概略構成を示す図である。図14において、1401はセキュリティコード送信部、1410はコンピュータ、1411はセキュリティコード受信部である。

【0140】図14に示す様に、本実施形態のコンピュ

ータ不正使用防止装置は、セキュリティコード送信部1401と、コンピュータ1410と、セキュリティコード受信部1411とを有している。

【0141】また、図14に示す様に、本実施形態のコンピュータ不正使用防止装置では、ネットワークを介して接続されたコンピュータ1410のセキュリティ管理を、コンピュータ110から行う構成を表している。

【0142】本実施形態のコンピュータ不正使用防止装置のコンピュータ110は、ネットワークを介してコンピュータ1410にセキュリティコードを送信するセキュリティコード送信部1401を備え、また、コンピュータ1410は、ネットワークを介してコンピュータ110から送信されたセキュリティコードを受信するセキュリティコード受信部1411を備えている。

【0143】図15は、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116の概略構成を示す図である。図15において、1501は他システム管理処理機能である。

【0144】図15に示す様に、本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116は、他システム管理処理機能1501を有している。

【0145】本実施形態のコンピュータ不正使用防止装置のセキュリティ管理処理部116は、実施形態1に示した複数の処理機能に加え、ネットワークを介して接続されたコンピュータ1410のセキュリティ管理を行う他システム管理処理機能1501を備えている。

【0146】本実施形態のコンピュータ不正使用防止装置では、セキュリティキー101から受信したセキュリティコードが有効なセキュリティコードである場合に、コンピュータ1410のセキュリティ管理を実行する他システム管理処理機能1501が選択されると、セキュリティコード送信部1401により、セキュリティキー101から受信済みの有効なセキュリティコードをネットワークに接続されたコンピュータ1410に送信する。

【0147】ネットワークに接続されたコンピュータ1410は、セキュリティコード受信部1411によりセキュリティコードを受信した後、コンピュータ1410のセキュリティ管理処理部116を起動する。

【0148】セキュリティコード送信部1401によりセキュリティコードを送信したコンピュータ110は、前記起動されたコンピュータ1410のセキュリティ管理処理部116に、セキュリティ管理に関する指示を送り、コンピュータ1410のセキュリティ管理機能を実行する。

【0149】以上説明した様に、本実施形態のコンピュータ不正使用防止装置によれば、ネットワークに接続された他のコンピュータのセキュリティ管理処理を実行するので、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュ

タに対してもセキュリティ管理を行うことが可能である。

【0150】以上、本発明を前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【0151】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【0152】(1)発生したユニークなセキュリティコードを出力してコンピュータのセキュリティ管理を行うので、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上することが可能である。

【0153】(2)コンピュータの信号出力装置により変更したセキュリティコードをセキュリティキーに出力し、セキュリティキーのセキュリティコードを変更するので、セキュリティの強度を向上せざるが可能である。

【0154】(3)ネットワークに接続された他のコンピュータのセキュリティ管理処理を実行するので、セキュリティキーからのセキュリティコード信号を入力するインタフェースを備えていないコンピュータに対してもセキュリティ管理を行うことが可能である。

【図面の簡単な説明】

【図1】実施形態1のコンピュータ不正使用防止装置の概略構成を示す図である。

【図2】実施形態1のコンピュータ不正使用防止装置のセキュリティ管理処理部116の概略構成を示す図である。

【図3】実施形態1のコンピュータ不正使用防止装置のセキュリティコードの登録処理の処理手順を示すフローチャートである。

【図4】実施形態1のコンピュータ不正使用防止装置のセキュリティコードの変更処理の処理手順を示すフローチャートである。

【図5】実施形態1のコンピュータ不正使用防止装置のシステム起動ロック処理の処理手順を示すフローチャートである。

【図6】実施形態1のコンピュータ不正使用防止装置の中断再開ロック処理の処理手順を示すフローチャートである。

【図7】実施形態1のコンピュータ不正使用防止装置の

アプリケーション起動ロック処理の処理手順を示すフローチャートである。

【図8】実施形態1のコンピュータ不正使用防止装置のファイルロック処理の処理手順を示すフローチャートである。

【図9】実施形態1のコンピュータ不正使用防止装置の暗号化処理の処理手順を示すフローチャートである。

【図10】実施形態1のコンピュータ不正使用防止装置の復号化処理の処理手順を示すフローチャートである。

【図11】実施形態1のコンピュータ不正使用防止装置の使用状況の履歴取得処理の処理手順を示すフローチャートである。

【図12】実施形態2のコンピュータ不正使用防止装置の概略構成を示す図である。

【図13】実施形態2のコンピュータ不正使用防止装置のセキュリティ管理処理部116の概略構成を示す図である。

【図14】実施形態3のコンピュータ不正使用防止装置の概略構成を示す図である。

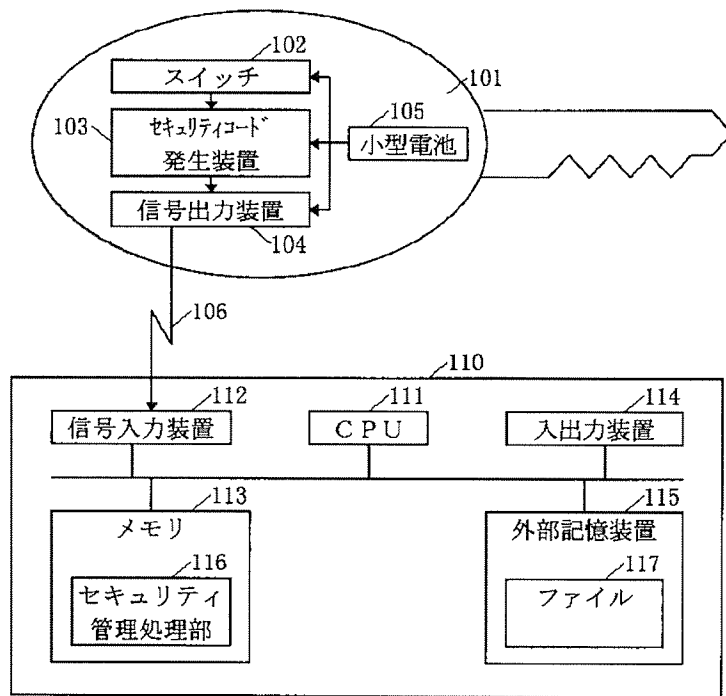
【図15】実施形態3のコンピュータ不正使用防止装置のセキュリティ管理処理部116の概略構成を示す図である。

【符号の説明】

101…セキュリティキー、102…スイッチ、103…セキュリティコード発生装置、104…信号出力装置、105…小型電池、106…セキュリティコード信号、110…コンピュータ、111…CPU、112…信号入力装置、113…メモリ、114…入出力装置、115…外部記憶装置、116…セキュリティ管理処理部、117…ファイル、201…登録処理機能、202…変更処理機能、203…システム起動ロック処理機能、204…中断再開ロック処理機能、205…アプリケーション起動ロック処理機能、206…ファイルロック処理機能、207…暗号化処理機能、208…復号化処理機能、209…使用状況の履歴取得処理機能、210…登録リスト、1200…セキュリティキー、1201…ICカード側信号入力装置、1210…ICカードリーダライタ、1211…ICカードリーダライタ側信号出力装置、1301…セキュリティコード変更処理機能、1401…セキュリティコード送信部、1410…コンピュータ、1411…セキュリティコード受信部、1501…他システム管理処理機能。

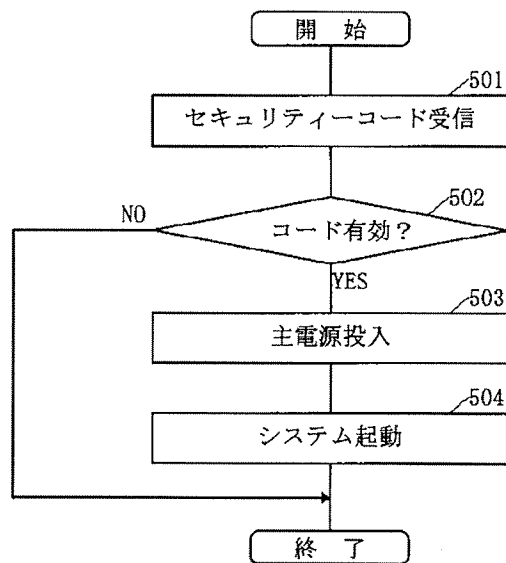
【図1】

図1



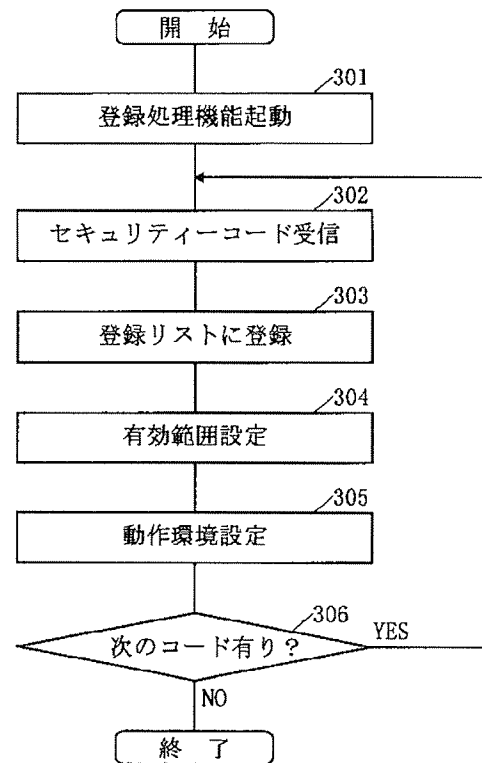
【図5】

図5



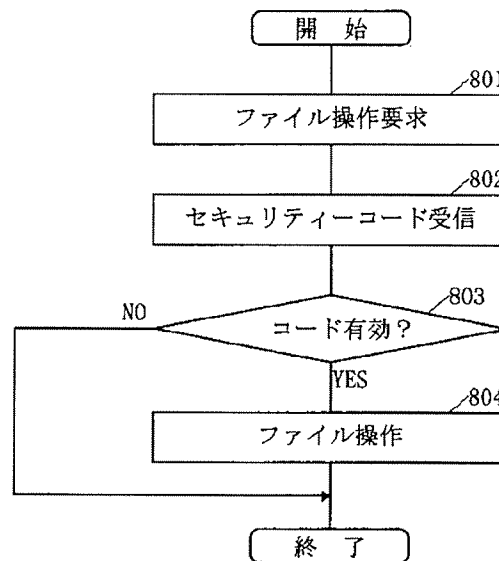
【図3】

図3



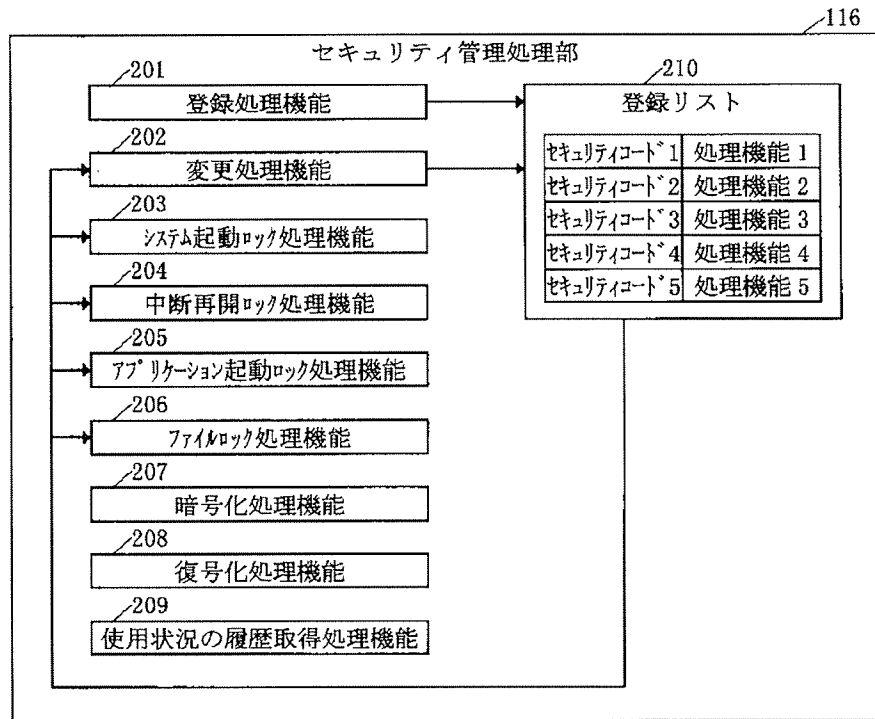
【図8】

図8



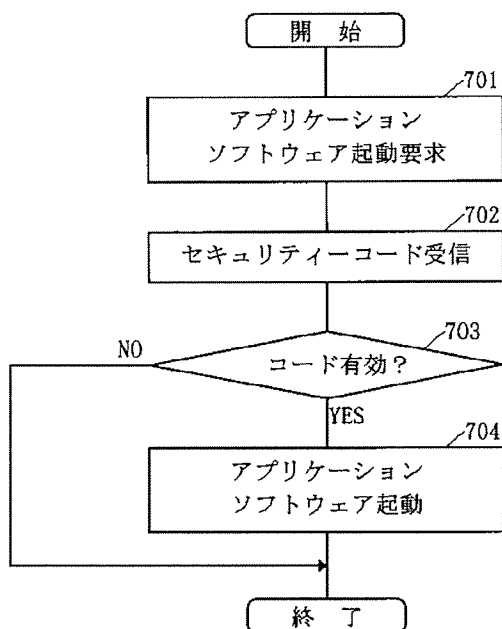
【図2】

図2



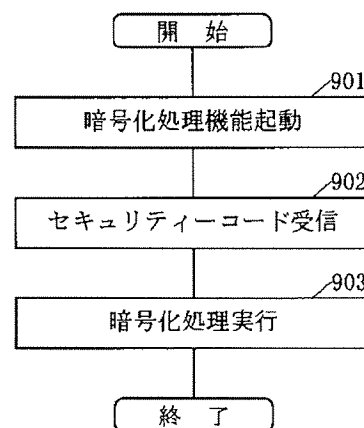
【図7】

図7



【図9】

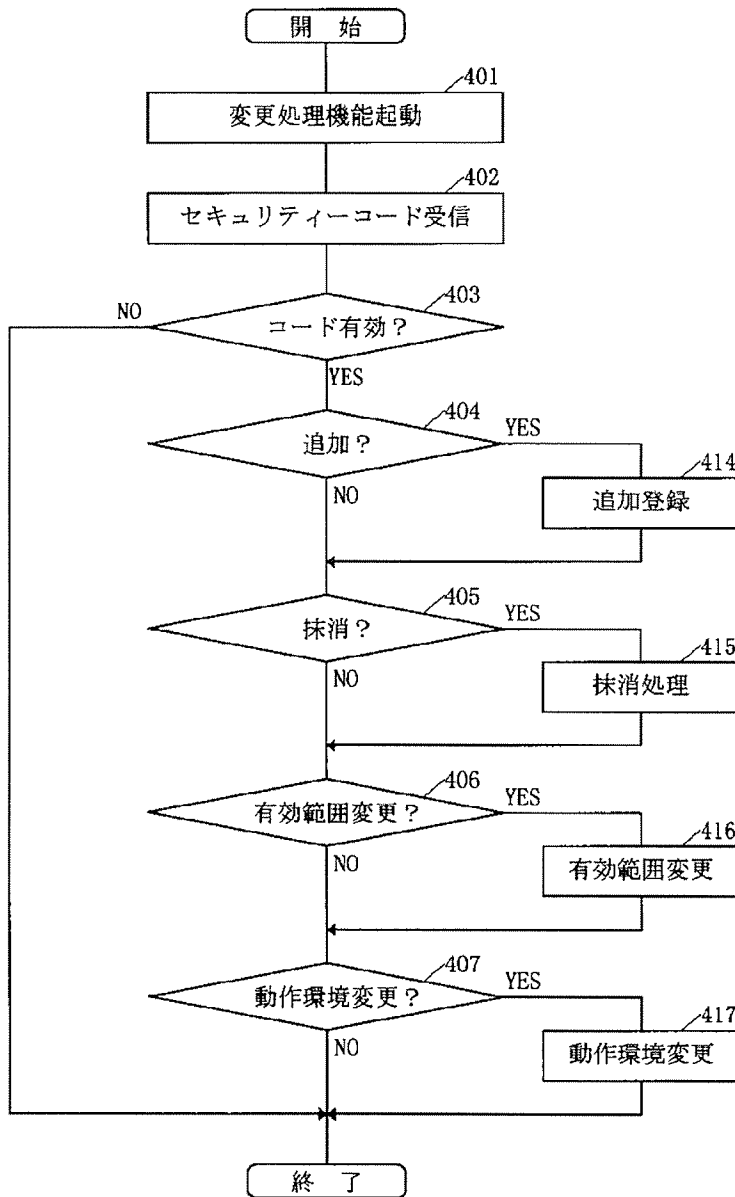
図9





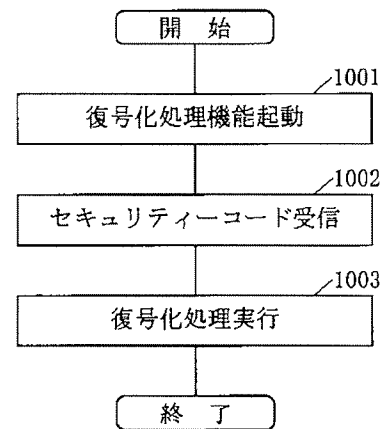
【図4】

図 4



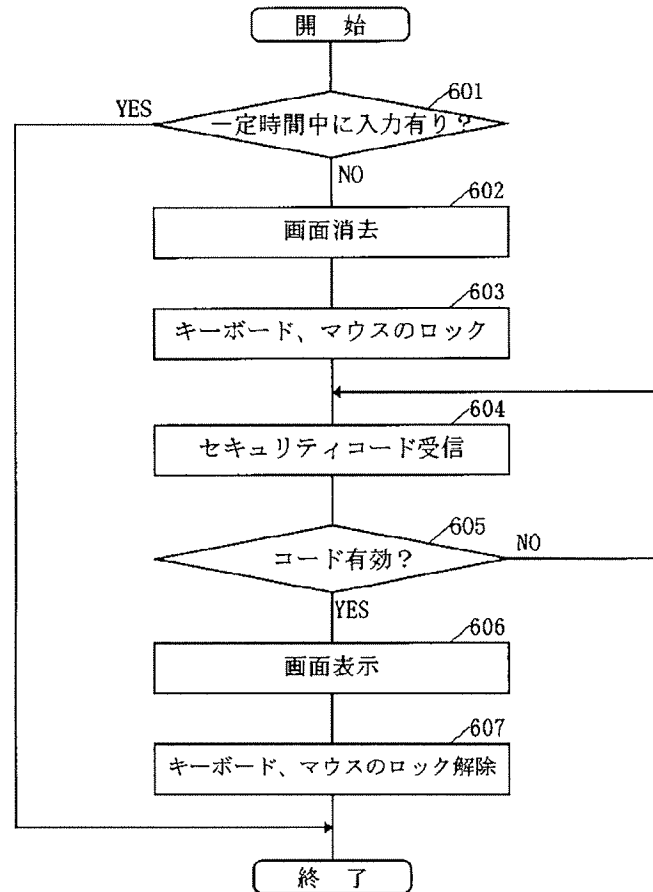
【図10】

図 10



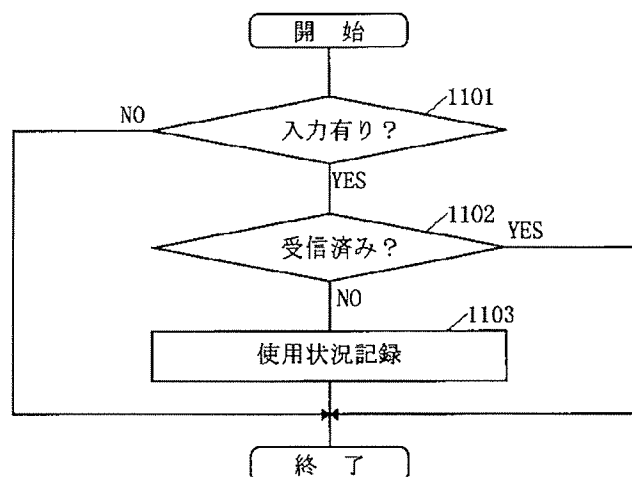
【図6】

図 6



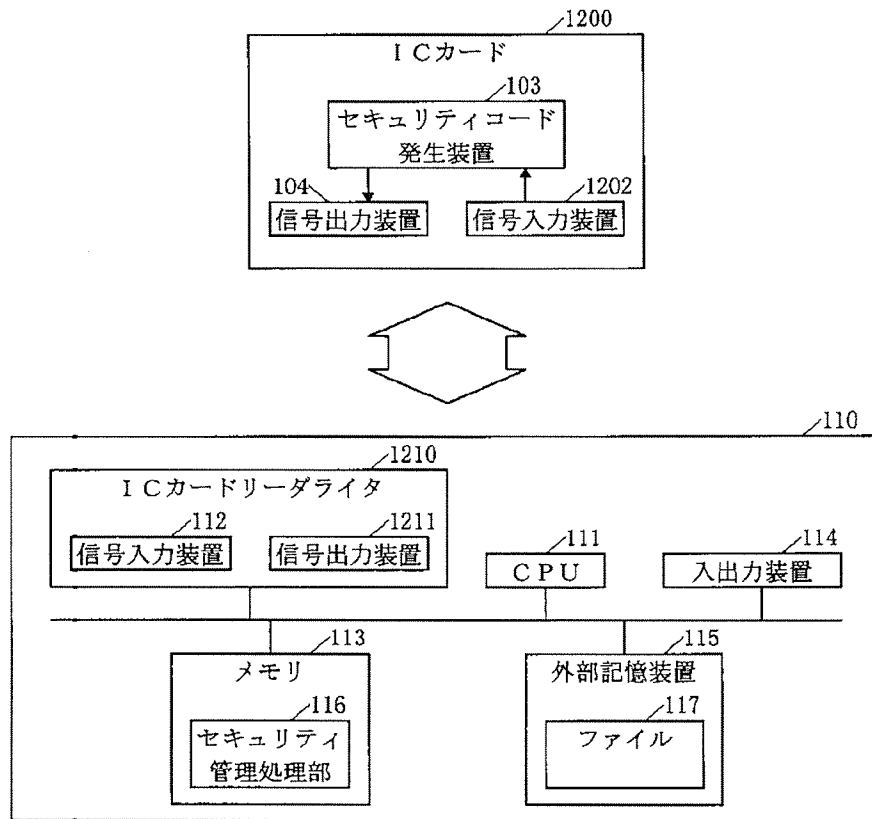
【図11】

図 11



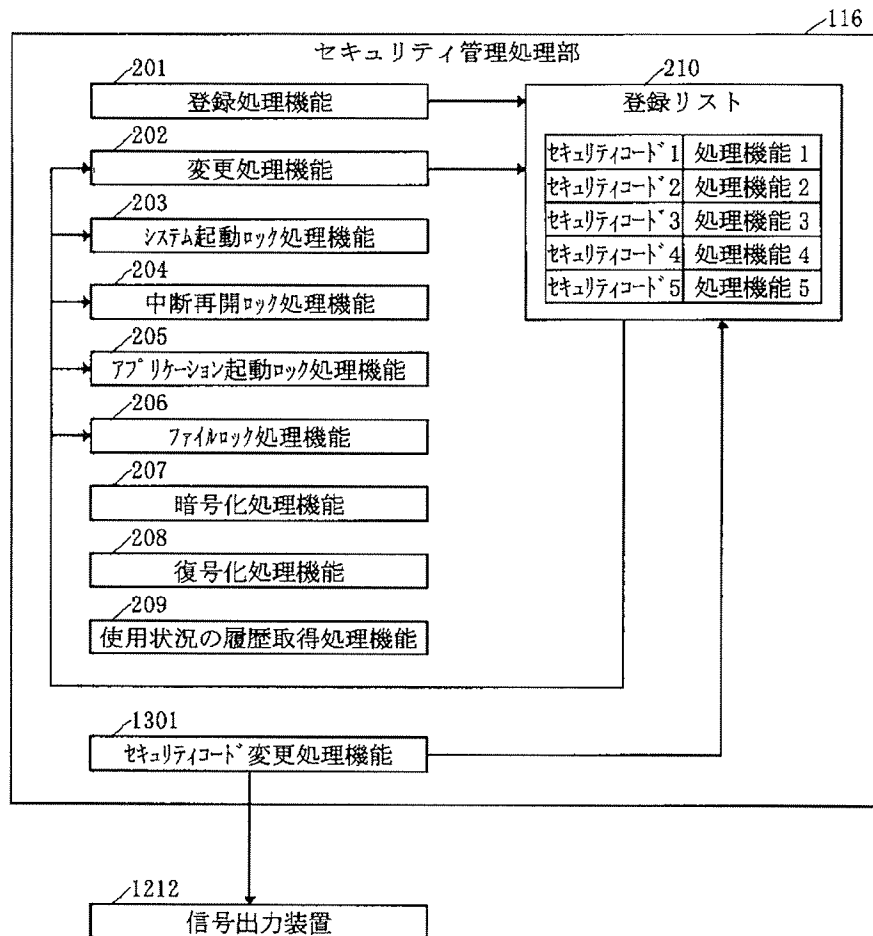
【図12】

図12



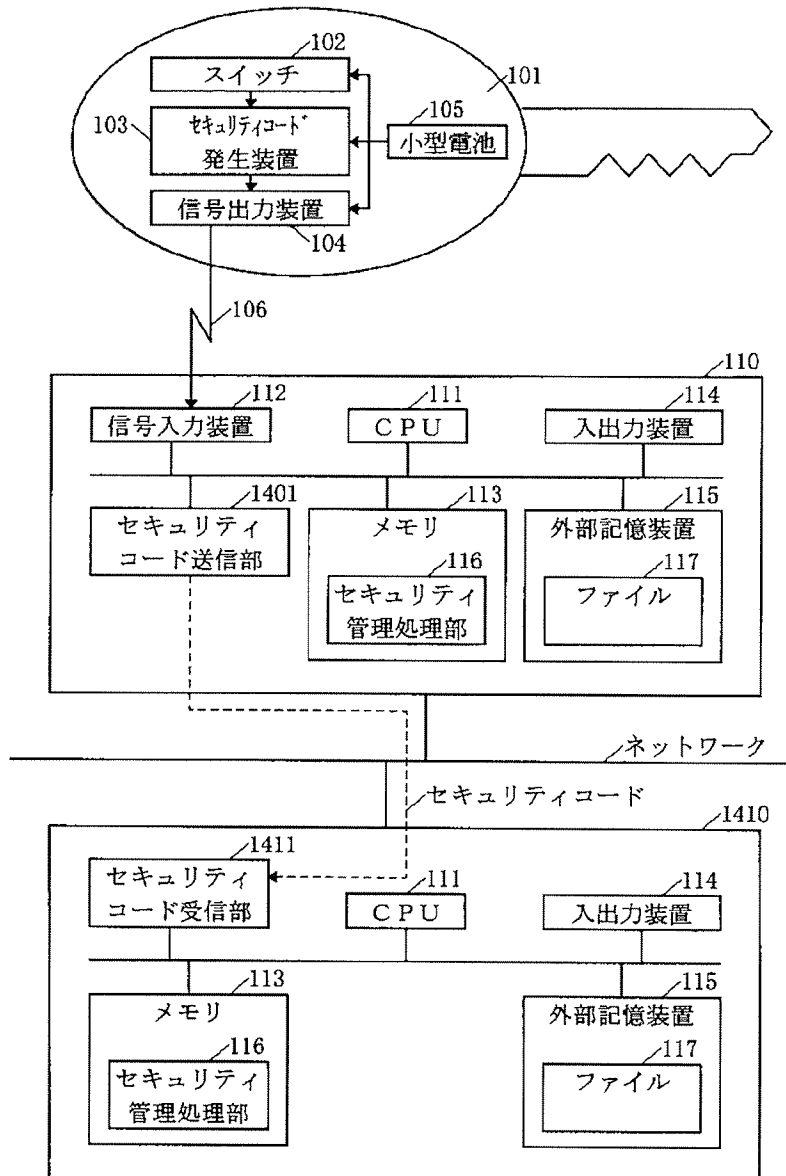
【図13】

図 1 3



【図14】

図14



【図15】

図 15

